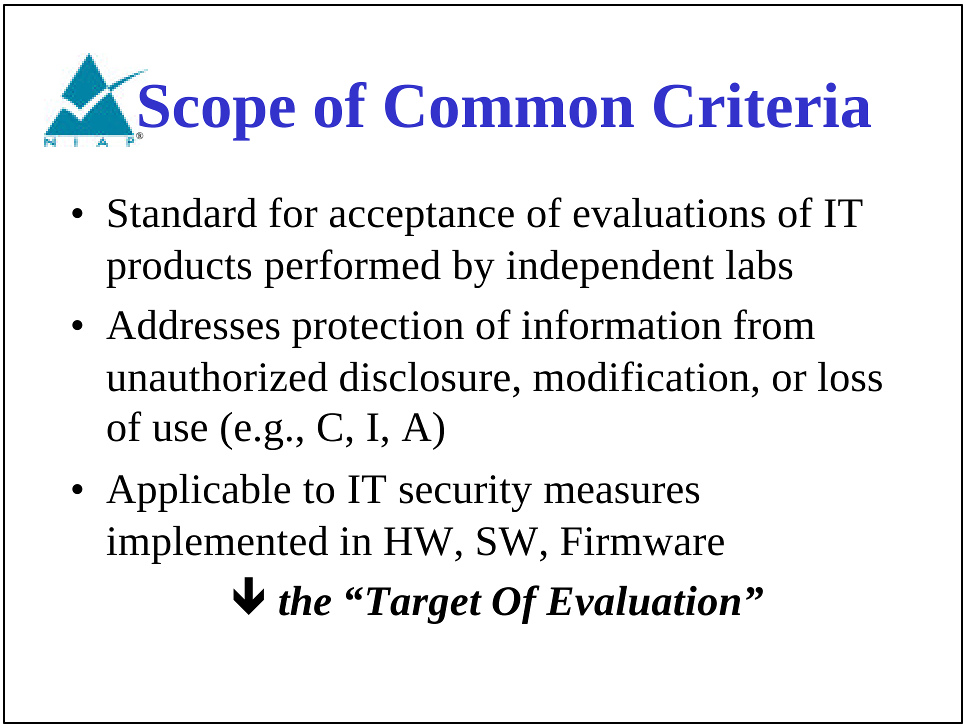
US
Canada
UK
Germany
France
Netherlands
Common Criteria

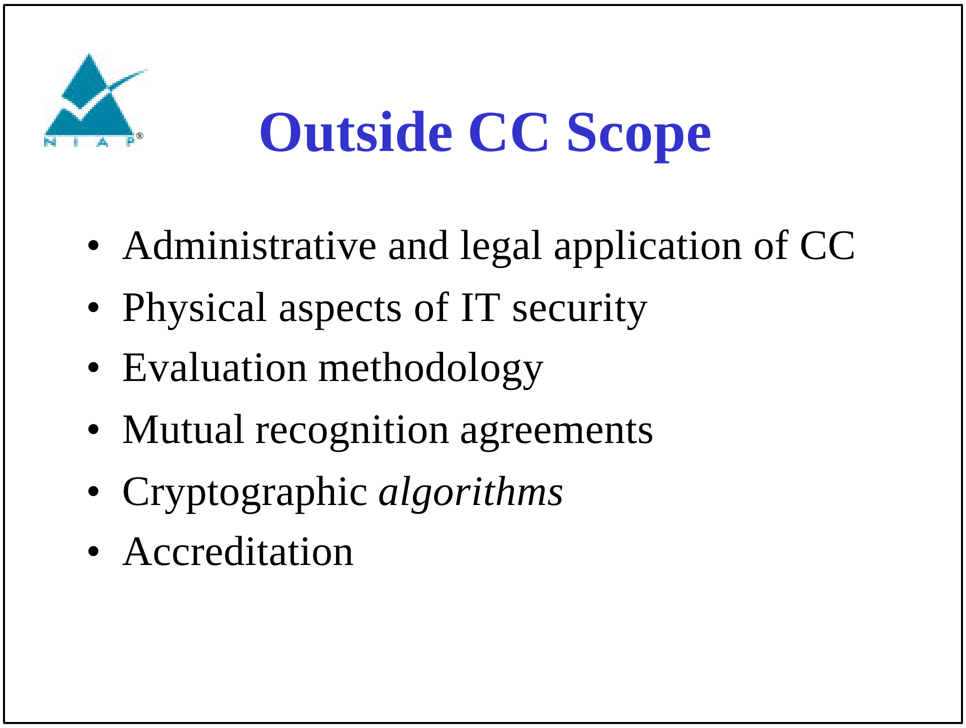
A collection of generic security requirements (statements) to aid in the specification of product/system security attributes (Functional and Assurance)



Scope of Common Criteria

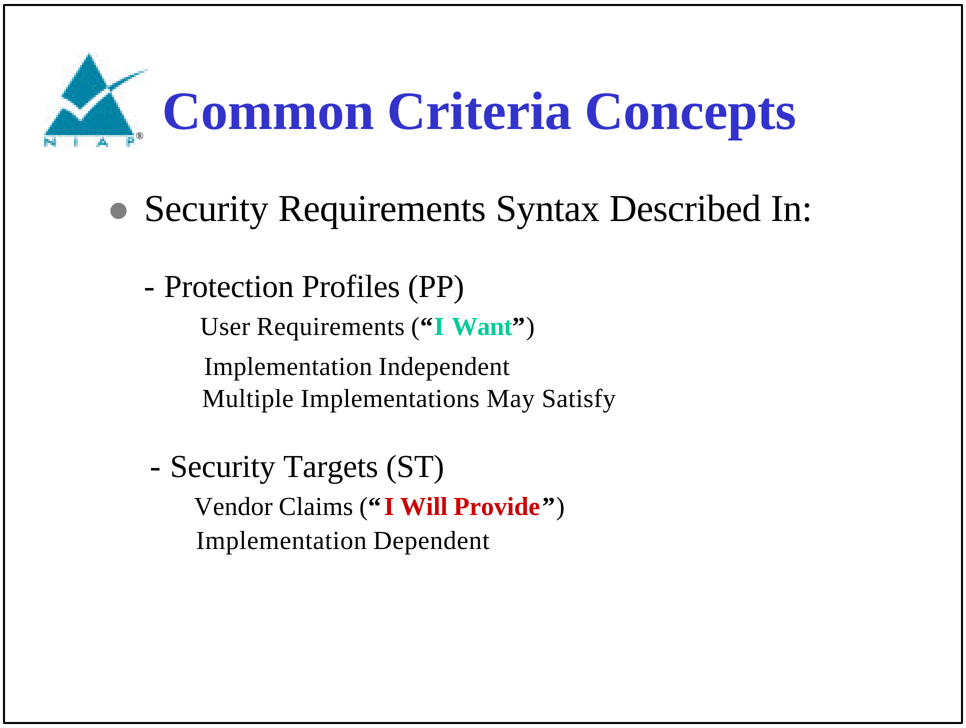
- Standard for acceptance of evaluations of IT products performed by independent labs
- Addresses protection of information from unauthorized disclosure, modification, or loss of use (e.g., C, I, A)
- Applicable to IT security measures implemented in HW, SW, Firmware

↓ ***the "Target Of Evaluation"***



Outside CC Scope

- Administrative and legal application of CC
- Physical aspects of IT security
- Evaluation methodology
- Mutual recognition agreements
- Cryptographic *algorithms*
- Accreditation



Common Criteria Concepts

- Security Requirements Syntax Described In:

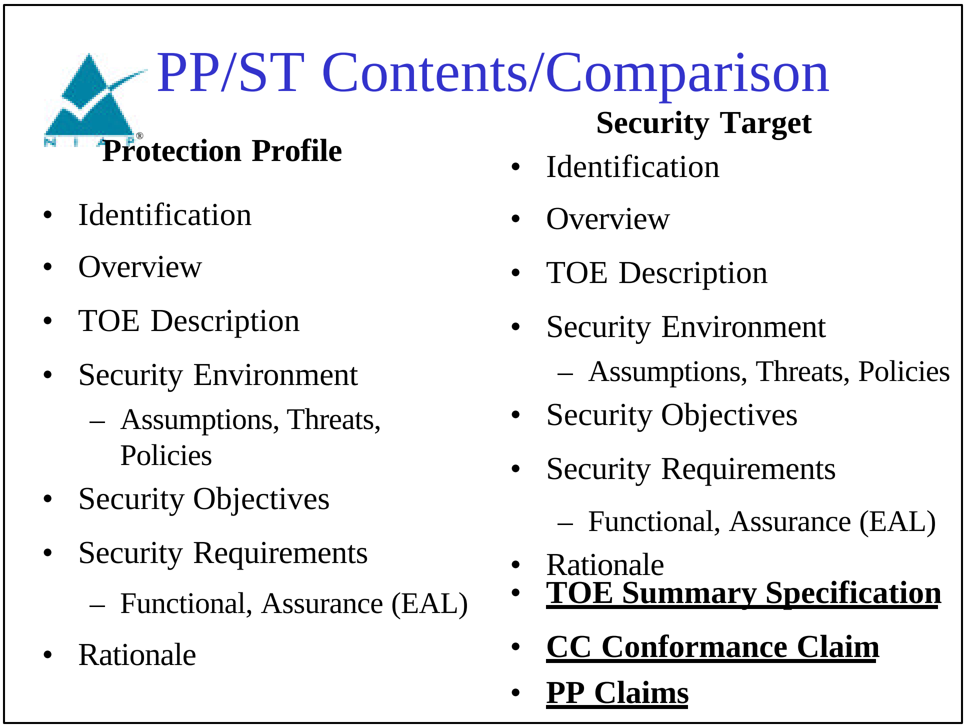
  - Protection Profiles (PP)

    User Requirements (“**I Want**”)

    Implementation Independent
    Multiple Implementations May Satisfy

  - Security Targets (ST)

    Vendor Claims (“**I Will Provide**”)
    Implementation Dependent



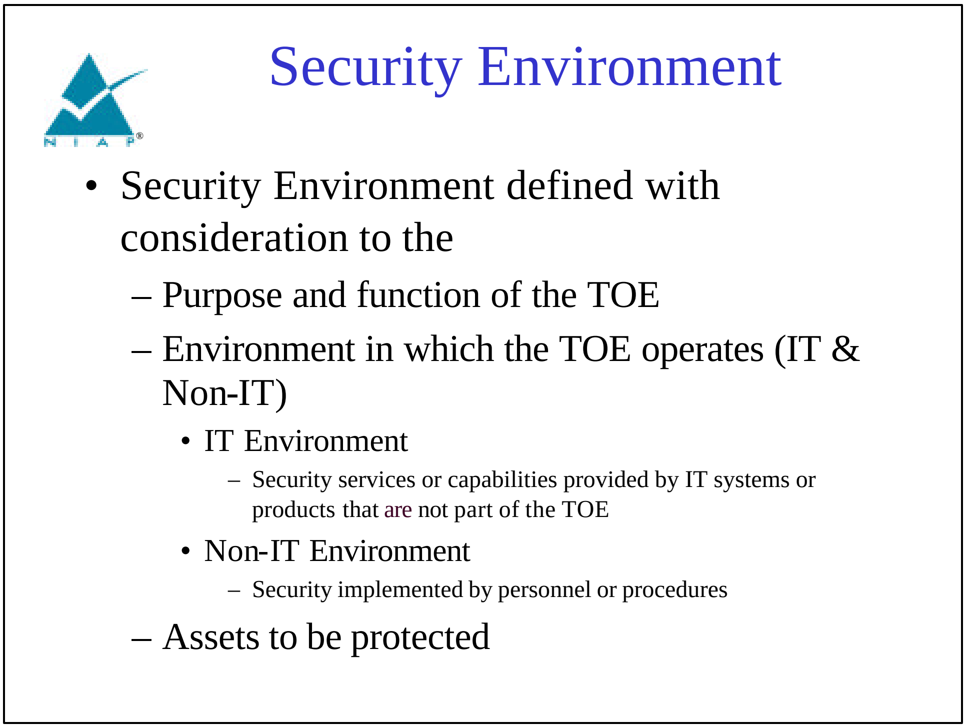
PP/ST Contents/Comparison

Protection Profile

- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale

Security Target

- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - Functional, Assurance (EAL)
- Rationale
- **TOE Summary Specification**
- **CC Conformance Claim**
- **PP Claims**



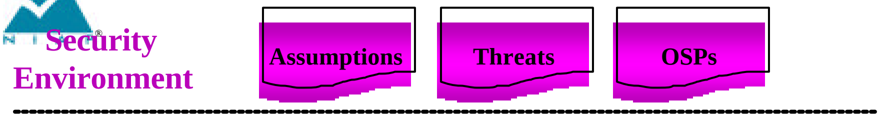
Security Environment

- Security Environment defined with consideration to the
  - Purpose and function of the TOE
  - Environment in which the TOE operates (IT & Non-IT)
    - IT Environment
      - Security services or capabilities provided by IT systems or products that are not part of the TOE
    - Non-IT Environment
      - Security implemented by personnel or procedures
  - Assets to be protected

Security Environment

- Assumptions
  - *The security aspects of the environment in which the TOE will be used or is intended to be used.*
- Threats
  - *The ability to exploit a vulnerability by a threat agent.*
- Organizational Security Policies (OSPs)
  - *A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations.*

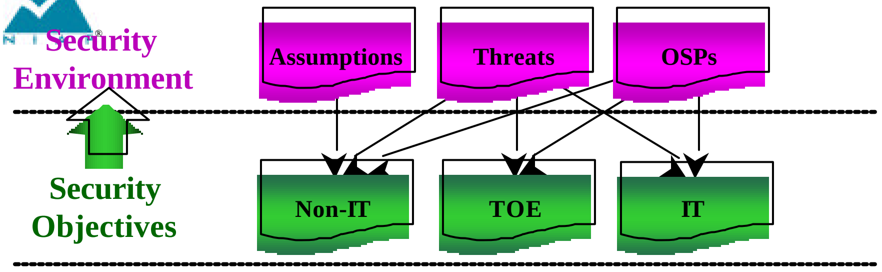
PP/ST Framework



Security Objectives

- Objectives establish the basis for the selection of security requirements (functional & assurance)
- Objective are completely based upon the statement of the Security Environment
- Objectives
  - – Support Assumptions
  - – Counter Threats (eliminate, minimize, monitor)
  - – Enforce Organizational Security Policies

PP/ST Framework



Security Environment

Assumptions

Threats

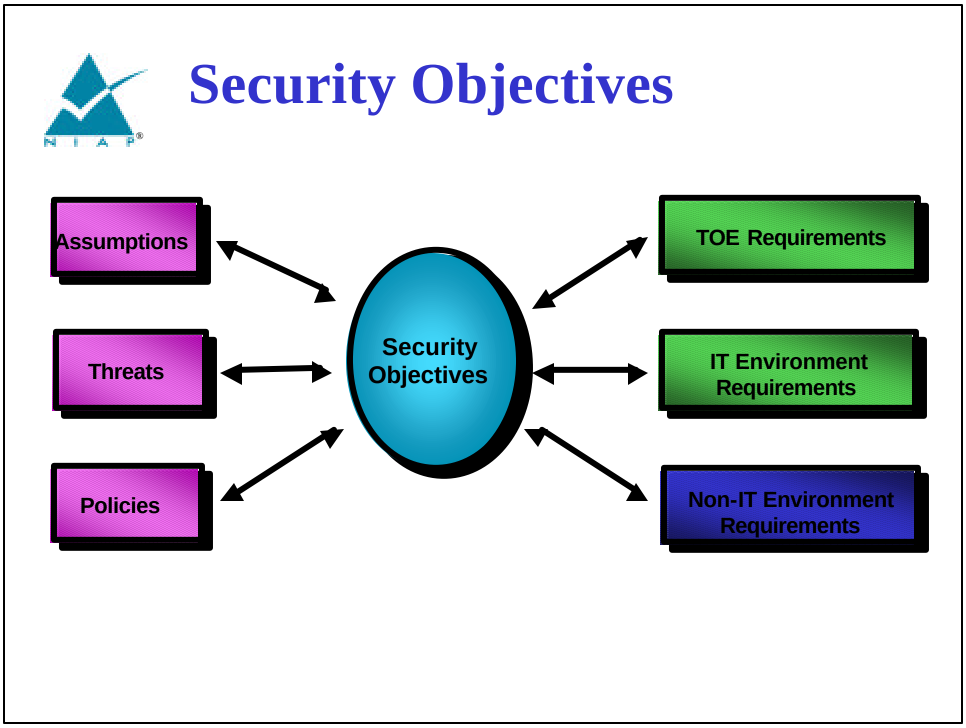
OSPs

Security Objectives

Non-IT

TOE

IT



Security Objectives

Assumptions

Threats

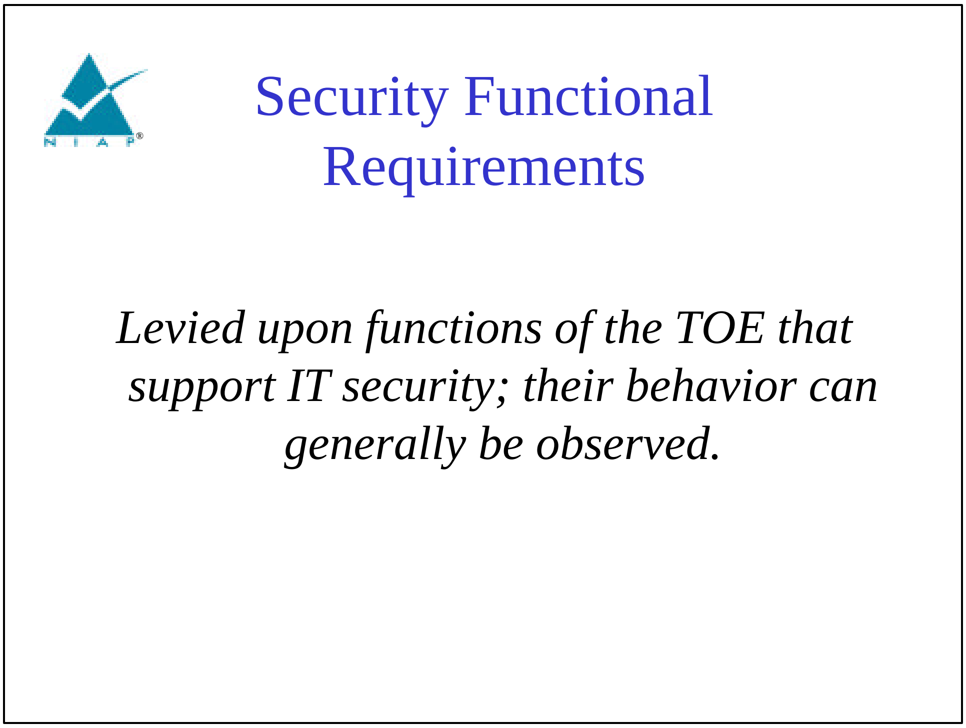
Policies

Security Objectives

TOE Requirements

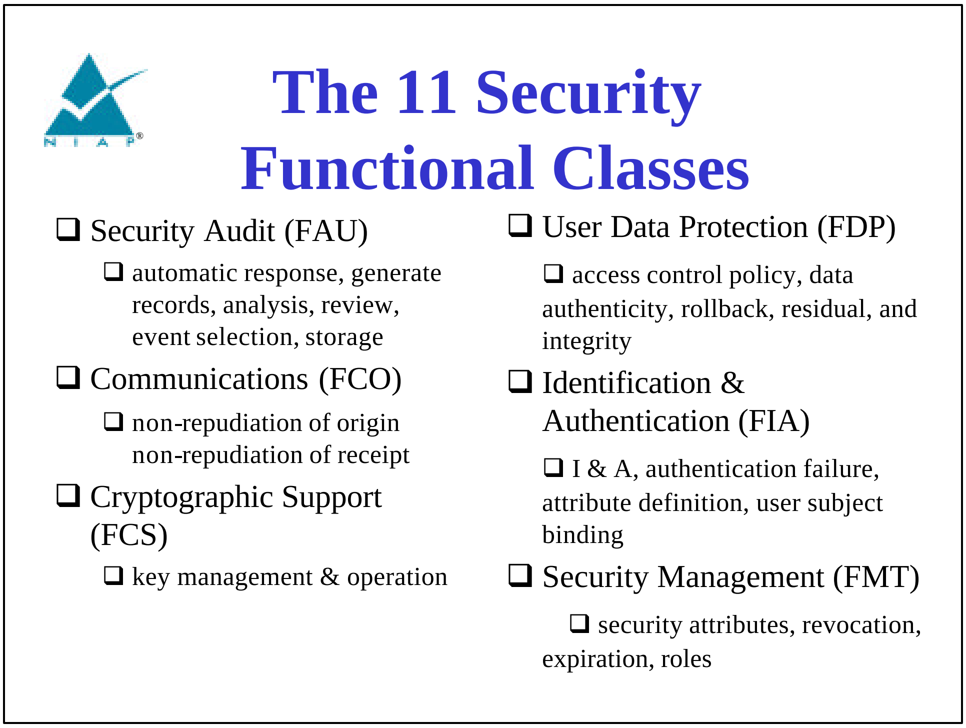
IT Environment Requirements

Non-IT Environment Requirements



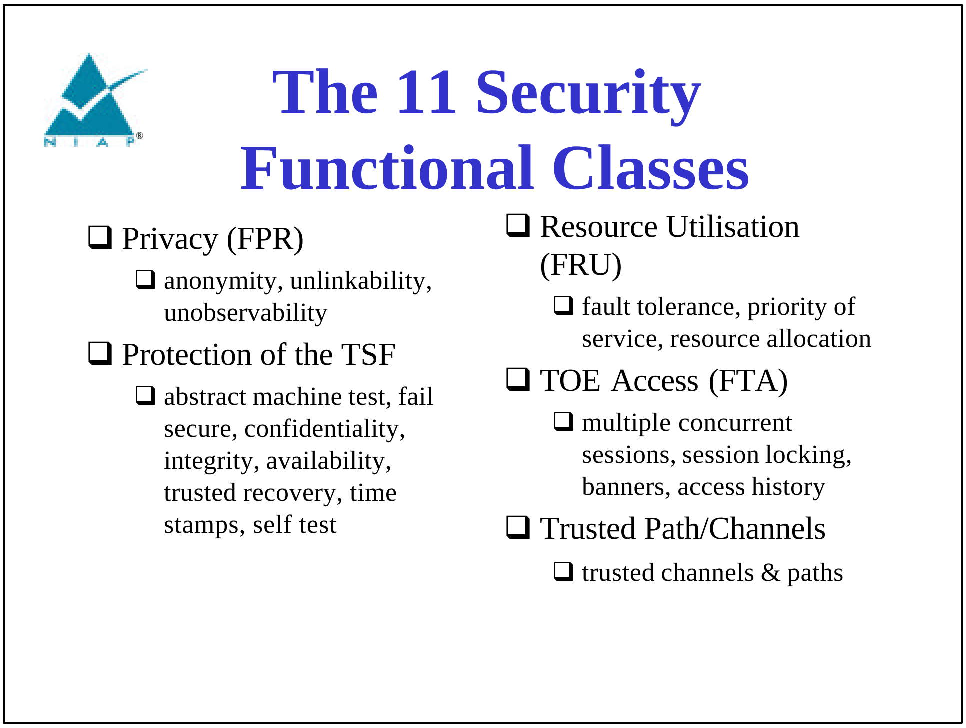
Security Functional Requirements

Levied upon functions of the TOE that support IT security; their behavior can generally be observed.



The 11 Security Functional Classes

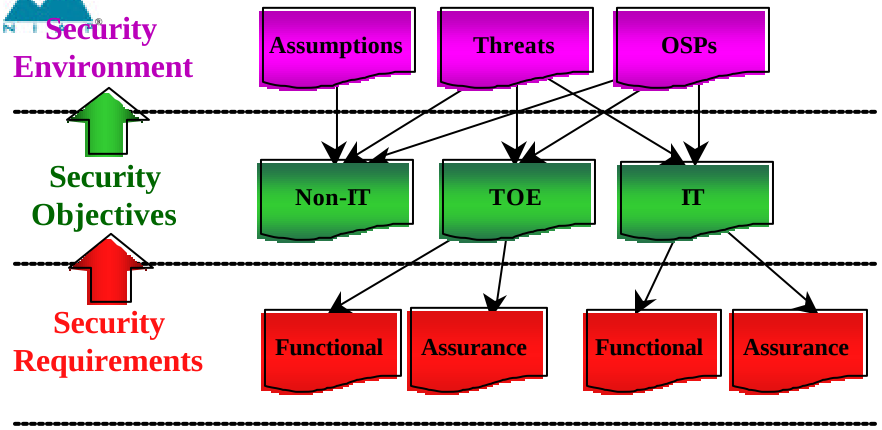
- ❑ Security Audit (FAU)
  - ❑ automatic response, generate records, analysis, review, event selection, storage
- ❑ Communications (FCO)
  - ❑ non-repudiation of origin non-repudiation of receipt
- ❑ Cryptographic Support (FCS)
  - ❑ key management & operation
- ❑ User Data Protection (FDP)
  - ❑ access control policy, data authenticity, rollback, residual, and integrity
- ❑ Identification & Authentication (FIA)
  - ❑ I & A, authentication failure, attribute definition, user subject binding
- ❑ Security Management (FMT)
  - ❑ security attributes, revocation, expiration, roles



The 11 Security Functional Classes

- ❑ Privacy (FPR)
  - ❑ anonymity, unlinkability, unobservability
- ❑ Protection of the TSF
  - ❑ abstract machine test, fail secure, confidentiality, integrity, availability, trusted recovery, time stamps, self test
- ❑ Resource Utilisation (FRU)
  - ❑ fault tolerance, priority of service, resource allocation
- ❑ TOE Access (FTA)
  - ❑ multiple concurrent sessions, session locking, banners, access history
- ❑ Trusted Path/Channels
  - ❑ trusted channels & paths

PP/ST Framework



Security Environment

Assumptions

Threats

OSPs

Security Objectives

Non-IT

TOE

IT

Security Requirements

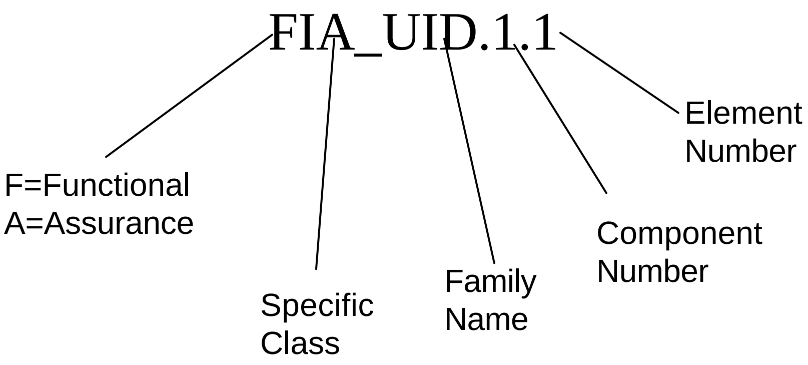
Functional

Assurance

Functional

Assurance

Interpreting Functional Requirement Names



FIA_UID.1.1

F=Functional
A=Assurance

Specific Class

Family Name

Component Number

Element Number

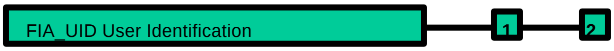
Functional Family Structure

FIA_UID User Identification

Family behavior

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

Component leveling



FIA_UID.1 Timing of identification, allows users to perform certain actions before being identified by the TSF.

FIA_UID.2 User identification before any action, require that users identify themselves before any action will be allowed by the TSF.

Functional Family Structure

FIA_UID.1 Timing of Identification

Hierarchical to: no other components.

FIA_UID.1.1 **The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.**

FIA_UID.1.2 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

Dependencies: **No dependencies**

FIA_UID.2 User Identification before any action

Hierarchical to: FIA.UID.1

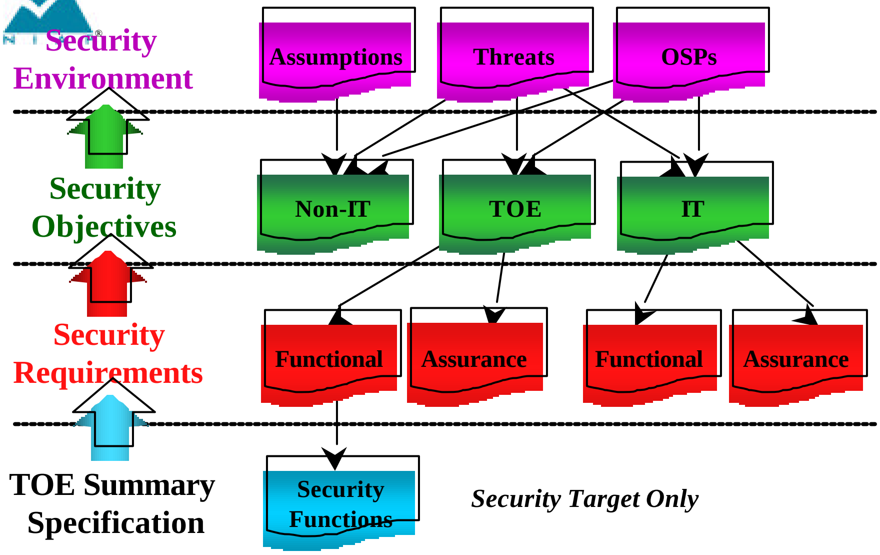
FIA_UID.2.1 **The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.**

Dependencies: **No dependencies**

Using Functional Components

- The CC defines 2 types of component relationships
  - – Dependency relationship - other component support (functional & assurance)
  - – Hierarchy relationship - between components within a class
- The CC provides 4 types of operations on functional components
  - – Assignment - “fill in the blank”
  - – Selection - “select from a list”
  - – Iteration - “repetitive use”
  - – Refinement - “tailor/modify”

PP/ST Framework



Security Environment

Assumptions

Threats

OSPs

Security Objectives

Non-IT

TOE

IT

Security Requirements

Functional

Assurance

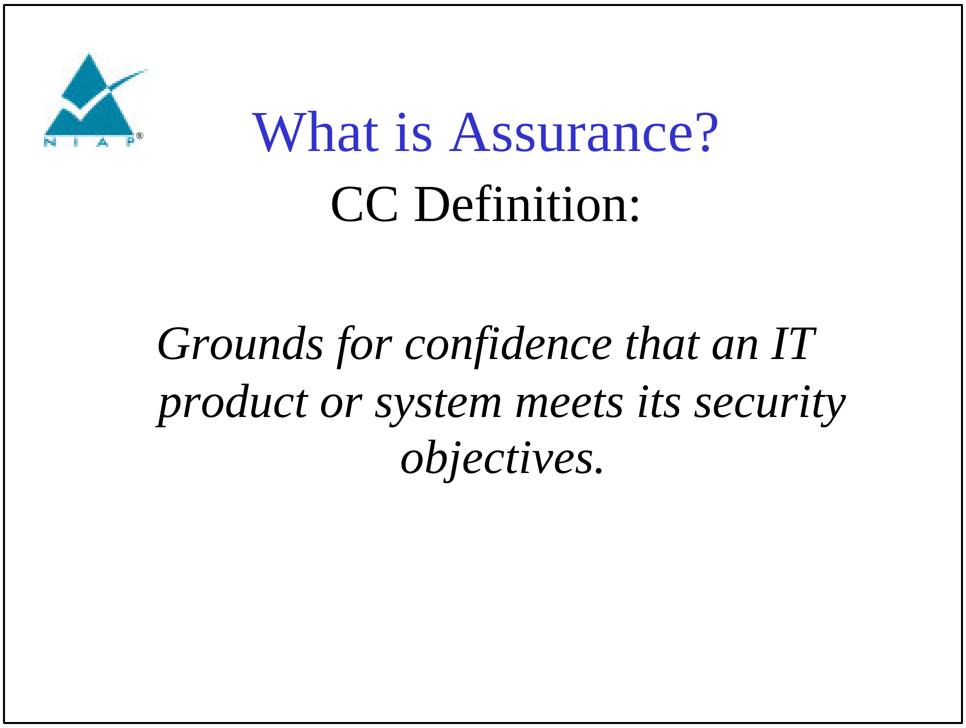
Functional

Assurance

TOE Summary Specification

Security Functions

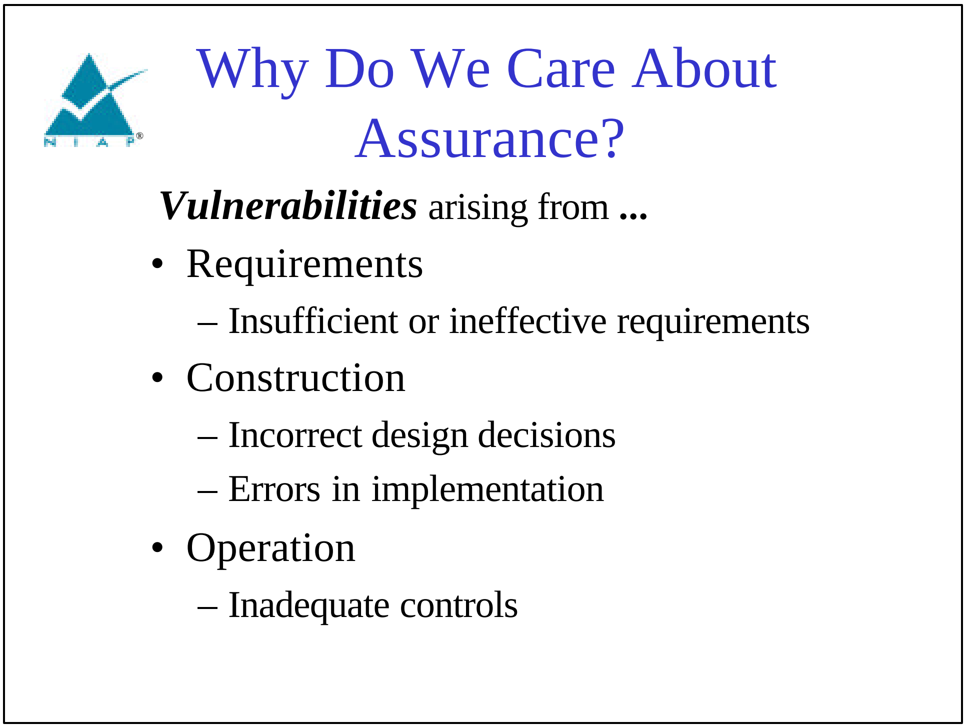
Security Target Only



What is Assurance?

CC Definition:

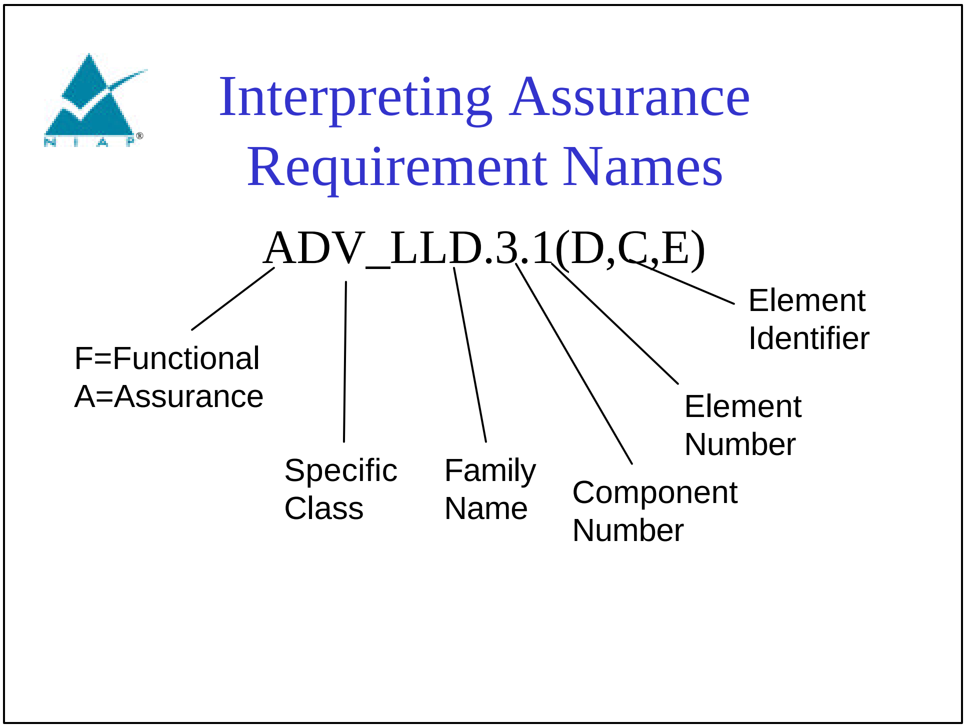
Grounds for confidence that an IT product or system meets its security objectives.



Why Do We Care About Assurance?

Vulnerabilities arising from **...**

- Requirements
  - – Insufficient or ineffective requirements
- Construction
  - – Incorrect design decisions
  - – Errors in implementation
- Operation
  - – Inadequate controls



Interpreting Assurance Requirement Names

ADV_LLD.3.1(D,C,E)

F=Functional
A=Assurance

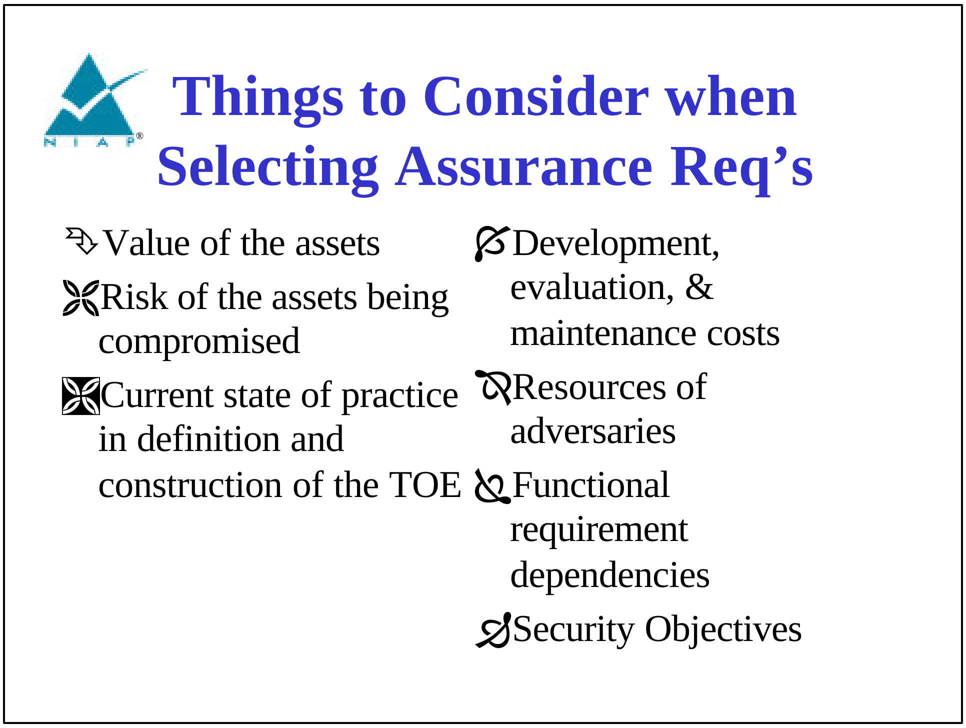
Specific Class

Family Name

Component Number

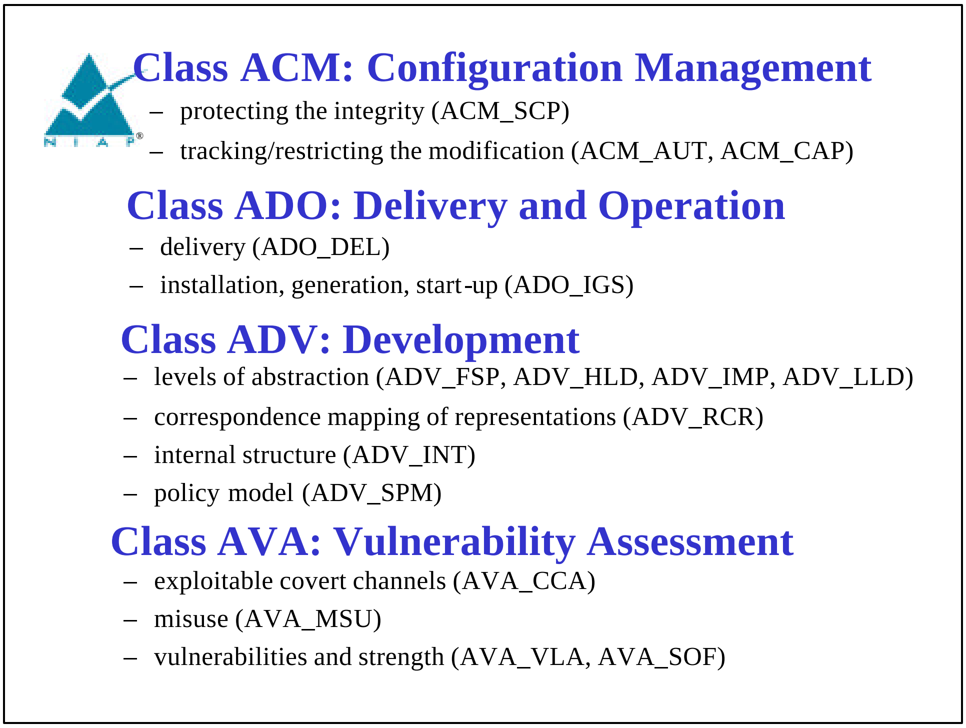
Element Number

Element Identifier



Things to Consider when Selecting Assurance Req's

- Value of the assets
- Risk of the assets being compromised
- Current state of practice in definition and construction of the TOE
- Development, evaluation, & maintenance costs
- Resources of adversaries
- Functional requirement dependencies
- Security Objectives



Class ACM: Configuration Management

- protecting the integrity (ACM_SCP)
- tracking/restricting the modification (ACM_AUT, ACM_CAP)

Class ADO: Delivery and Operation

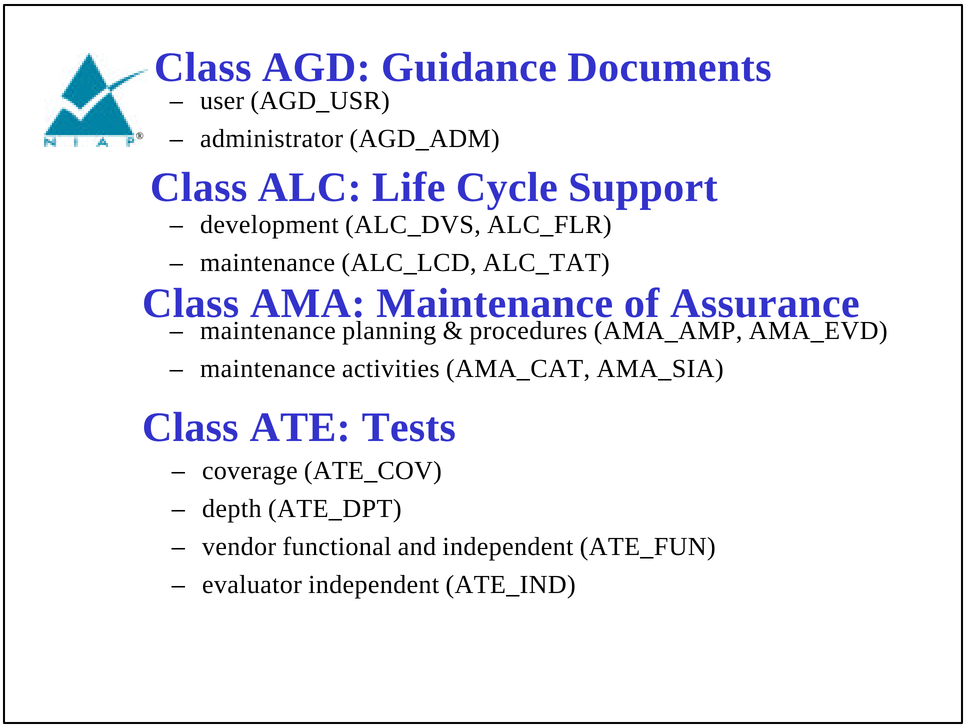
- delivery (ADO_DEL)
- installation, generation, start-up (ADO_IGS)

Class ADV: Development

- levels of abstraction (ADV_FSP, ADV_HLD, ADV_IMP, ADV_LLD)
- correspondence mapping of representations (ADV_RCR)
- internal structure (ADV_INT)
- policy model (ADV_SPM)

Class AVA: Vulnerability Assessment

- exploitable covert channels (AVA_CCA)
- misuse (AVA_MSU)
- vulnerabilities and strength (AVA_VLA, AVA_SOF)



Class AGD: Guidance Documents

- user (AGD_USR)
- administrator (AGD_ADM)

Class ALC: Life Cycle Support

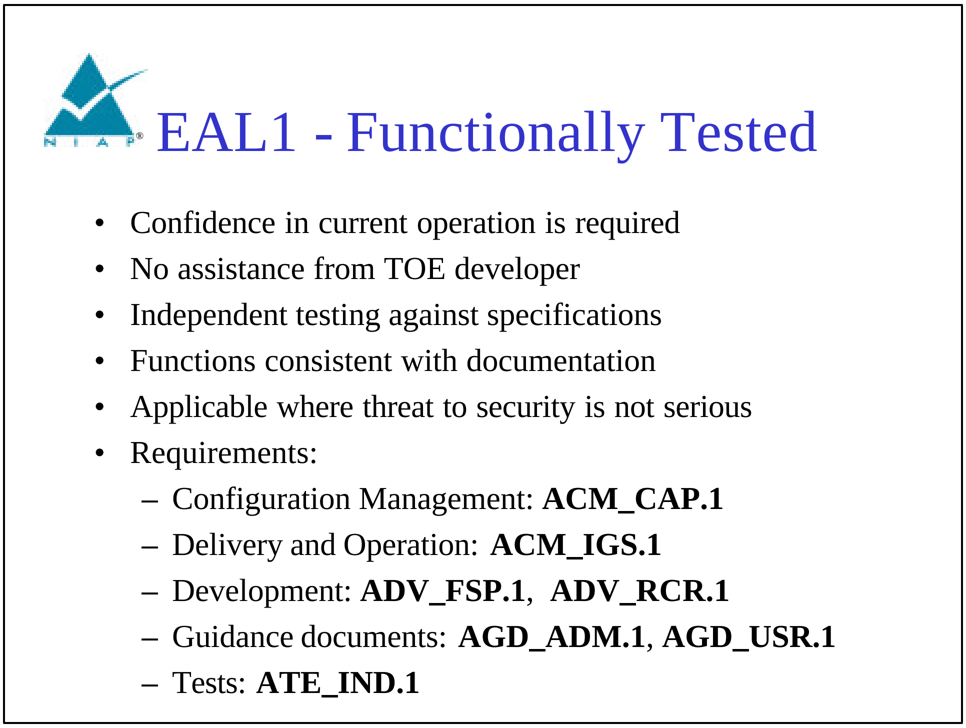
- development (ALC_DVS, ALC_FLR)
- maintenance (ALC_LCD, ALC_TAT)

Class AMA: Maintenance of Assurance

- maintenance planning & procedures (AMA_AMP, AMA_EVD)
- maintenance activities (AMA_CAT, AMA_SIA)

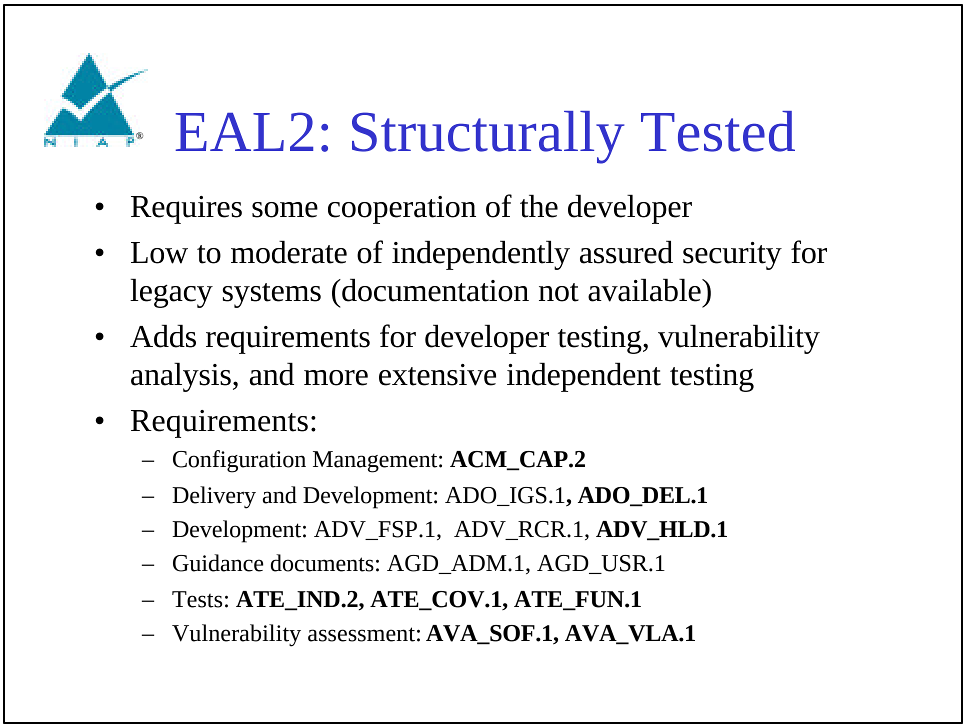
Class ATE: Tests

- coverage (ATE_COV)
- depth (ATE_DPT)
- vendor functional and independent (ATE_FUN)
- evaluator independent (ATE_IND)



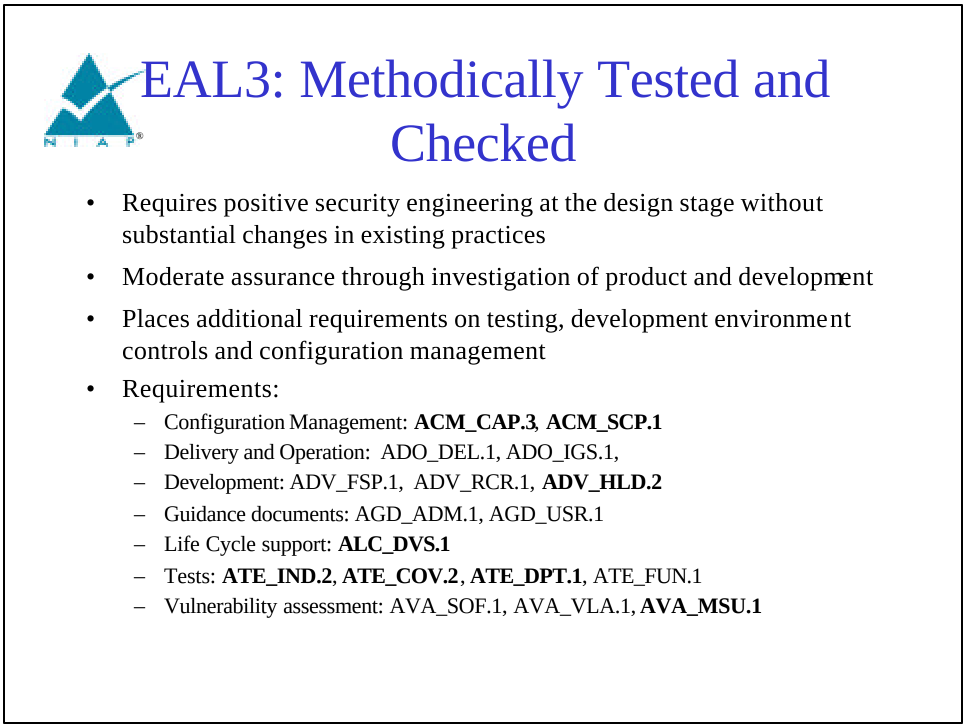
EAL1 - Functionally Tested

- Confidence in current operation is required
- No assistance from TOE developer
- Independent testing against specifications
- Functions consistent with documentation
- Applicable where threat to security is not serious
- Requirements:
  - Configuration Management: **ACM_CAP.1**
  - Delivery and Operation: **ACM_IGS.1**
  - Development: **ADV_FSP.1**, **ADV_RCR.1**
  - Guidance documents: **AGD_ADM.1**, **AGD_USR.1**
  - Tests: **ATE_IND.1**



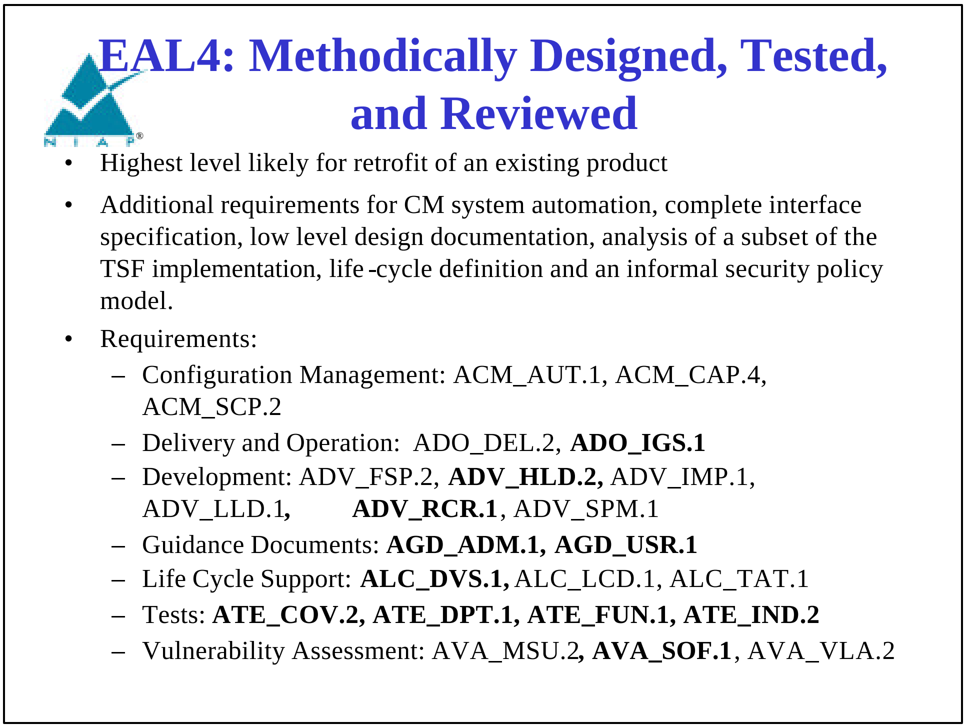
EAL2: Structurally Tested

- Requires some cooperation of the developer
- Low to moderate of independently assured security for legacy systems (documentation not available)
- Adds requirements for developer testing, vulnerability analysis, and more extensive independent testing
- Requirements:
  - Configuration Management: **ACM_CAP.2**
  - Delivery and Development: ADO_IGS.1**, ADO_DEL.1**
  - Development: ADV_FSP.1, ADV_RCR.1, **ADV_HLD.1**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Tests: **ATE_IND.2, ATE_COV.1, ATE_FUN.1**
  - Vulnerability assessment: **AVA_SOF.1, AVA_VLA.1**



EAL3: Methodically Tested and Checked

- Requires positive security engineering at the design stage without substantial changes in existing practices
- Moderate assurance through investigation of product and development
- Places additional requirements on testing, development environment controls and configuration management
- Requirements:
  - Configuration Management: **ACM_CAP.3**, **ACM_SCP.1**
  - Delivery and Operation: ADO_DEL.1, ADO_IGS.1,
  - Development: ADV_FSP.1, ADV_RCR.1, **ADV_HLD.2**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: **ALC_DVS.1**
  - Tests: **ATE_IND.2**, **ATE_COV.2**, **ATE_DPT.1**, ATE_FUN.1
  - Vulnerability assessment: AVA_SOF.1, AVA_VLA.1, **AVA_MSU.1**



EAL4: Methodically Designed, Tested, and Reviewed

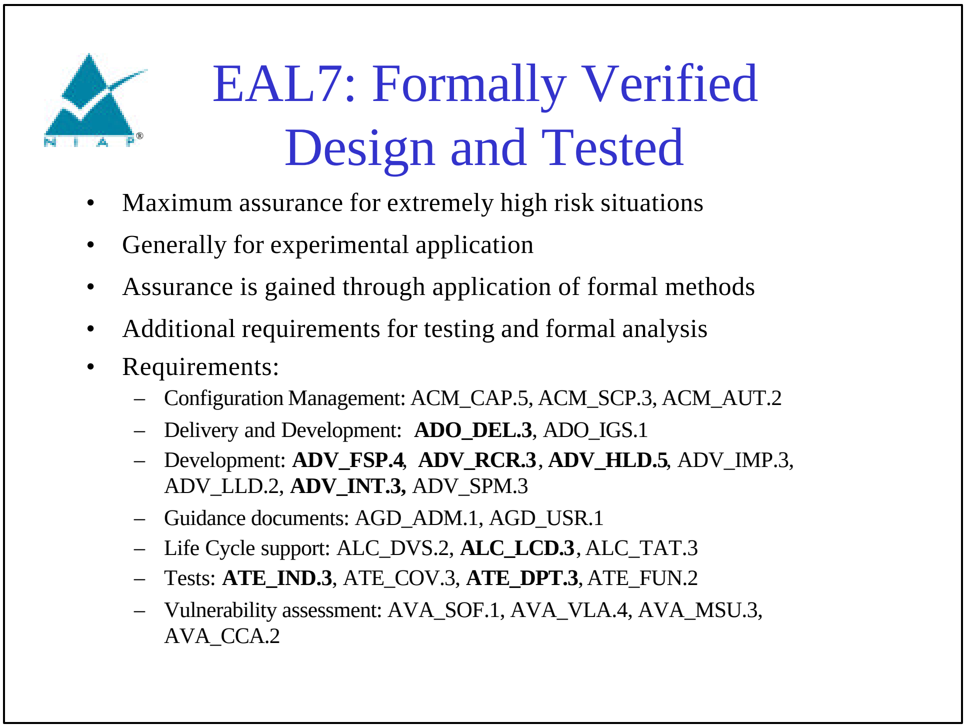
- Highest level likely for retrofit of an existing product
- Additional requirements for CM system automation, complete interface specification, low level design documentation, analysis of a subset of the TSF implementation, life -cycle definition and an informal security policy model.
- Requirements:
  - Configuration Management: ACM_AUT.1, ACM_CAP.4, ACM_SCP.2
  - Delivery and Operation: ADO_DEL.2, **ADO_IGS.1**
  - Development: ADV_FSP.2, **ADV_HLD.2,** ADV_IMP.1, ADV_LLD.1**,** **ADV_RCR.1**, ADV_SPM.1
  - Guidance Documents: **AGD_ADM.1, AGD_USR.1**
  - Life Cycle Support: **ALC_DVS.1,** ALC_LCD.1, ALC_TAT.1
  - Tests: **ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2**
  - Vulnerability Assessment: AVA_MSU.2**, AVA_SOF.1**, AVA_VLA.2

EAL5: Semiformally Designed and Tested

- High assurance, risk situations
- Requires rigorous commercial development practices and moderate use of specialist engineering techniques
- Additional requirements on specification, design, and their correspondence
- Requirements:
  - Configuration Management: ACM_CAP.4, **ACM_SCP.3**, ACM_AUT.1
  - Delivery and Development: ADO_DEL.2, ADO_IGS.1
  - Development: **ADV_FSP.3**, **ADV_RCR.2**, **ADV_HLD.3**, **ADV_IMP.2**, ADV_LLD.1, **ADV_INT.1, ADV_SPM.3**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: ALC_DVS.1, **ALC_LCD.2**, **ALC_TAT.2**
  - Tests: ATE_IND.2, ATE_COV.2, **ATE_DPT.2**, ATE_FUN.1
  - Vulnerability assessment: AVA_SOF.1, **AVA_VLA.3**, AVA_MSU.2, **AVA_CCA.1**

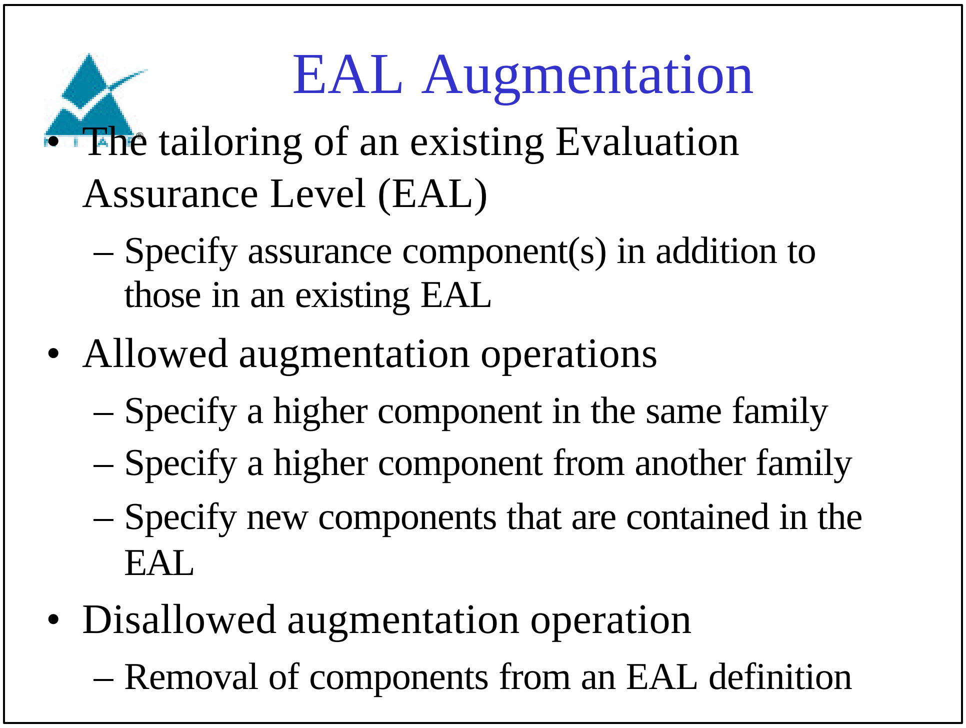
EAL6: Semiformally Verified Design and Tested

- Applicable to a rigorous development environment
- High Assurance for high value assets/risk situations
- Additional requirements on analysis, design, development, configuration management, vulnerability/covert channel analysis
- Requirements:
  - Configuration Management: **ACM_CAP.5**, ACM_SCP.3, **ACM_AUT.2**
  - Delivery and Development: ADO_DEL.2, ADO_IGS.1
  - Development: ADV_FSP.3, ADV_RCR.2, **ADV_HLD.4**, **ADV_IMP.3**, **ADV_LLD.2**, **ADV_INT.2,** ADV_SPM.3
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: **ALC_DVS.2**, ALC_LCD.2, **ALC_TAT.3**
  - Tests: ATE_IND.2, **ATE_COV.3**, ATE_DPT.2, **ATE_FUN.2**
  - Vulnerability assessment: AVA_SOF.1, **AVA_VLA.4**, **AVA_MSU.3**, **AVA_CCA.2**



EAL7: Formally Verified Design and Tested

- Maximum assurance for extremely high risk situations
- Generally for experimental application
- Assurance is gained through application of formal methods
- Additional requirements for testing and formal analysis
- Requirements:
  - Configuration Management: ACM_CAP.5, ACM_SCP.3, ACM_AUT.2
  - Delivery and Development: **ADO_DEL.3**, ADO_IGS.1
  - Development: **ADV_FSP.4**, **ADV_RCR.3**, **ADV_HLD.5**, ADV_IMP.3, ADV_LLD.2, **ADV_INT.3,** ADV_SPM.3
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: ALC_DVS.2, **ALC_LCD.3**, ALC_TAT.3
  - Tests: **ATE_IND.3**, ATE_COV.3, **ATE_DPT.3**, ATE_FUN.2
  - Vulnerability assessment: AVA_SOF.1, AVA_VLA.4, AVA_MSU.3, AVA_CCA.2

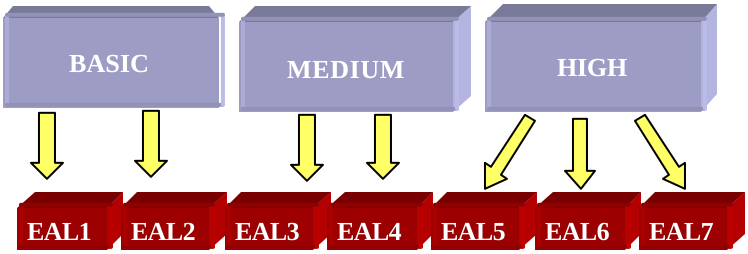


EAL Augmentation

- The tailoring of an existing Evaluation Assurance Level (EAL)
  - Specify assurance component(s) in addition to those in an existing EAL
- Allowed augmentation operations
  - Specify a higher component in the same family
  - Specify a higher component from another family
  - Specify new components that are contained in the EAL
- Disallowed augmentation operation
  - Removal of components from an EAL definition

DoD CIO Guidance and Policy Memorandum No. 6-8510

LEVELS OF CONCERN/ROBUSTNESS



BASIC

MEDIUM

HIGH

EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7

Common Criteria®

QUESTIONS?

Visit our Internet Websites:

http://www.nstissc.gov/html/library.html (NSTISSP No. 11)
http://www.c3i.osd.mil/org/cio/gpmlinks.html (GIG Guidance)
http://csrc.nist.gov/cc (Common Criteria)
http://www.radium.ncsc.mil/tpep/ (NSA Certified Products)
http://niap.nist.gov/cc-scheme (All Validated Products)
http://www.iatf.net (Draft Protection Profiles)